PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-165377
(43)Date of publication of application : 16.06.2000

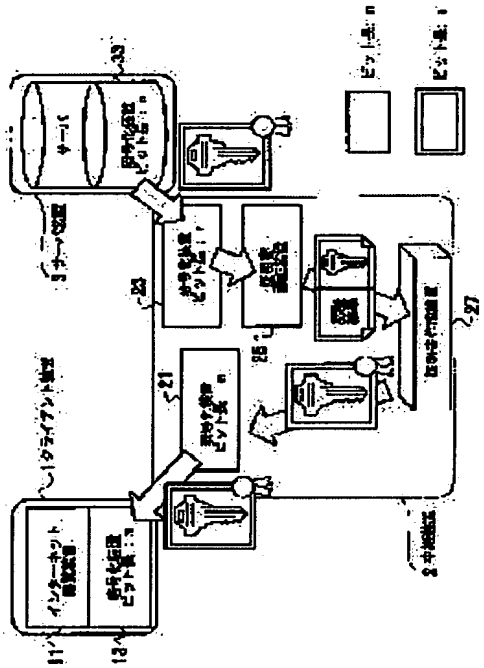
(51)Int.Cl. H04L 9/14
G06F 13/00
G09C 1/00
H04L 9/32

(21)Application number : 10-340635
(22)Date of filing : 30.11.1998

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : FUKAZAWA HIROAKI
MOTODA TOSHIHIRO

(54) ENCRYPTION PROTOCOL CONVERTER, ENCRYPTION PROTOCOL CONVERTING METHOD AND RECORDING MEDIUM RECORDING ENCRYPTION PROTOCOL CONVERSION PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an encryption protocol converter that enhances security for information transmission reception furthermore and can precisely authenticate a communication opposite party, and to provide an encryption protocol conversing method and a recording medium recording an encryption protocol conversion program.
SOLUTION: Encryption devices 21, 23 of an intermediate device 2 encrypt furthermore encrypted information sent/received between a client device 1 and a server device 3 so as to enhance the security, and a certificate authentication device 25 of the intermediate device 2 authenticates a certificate added to the encrypted information received from the server device 3, a certificate generator 27 generates a new certificate on the basis of the authentication result and the generated certificate is transmitted to the client device 1.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－165377
（P2000－165377A）
(43)公開日　平成12年６月16日(2000.6.16)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｈ０４Ｌ　9/14		Ｈ０４Ｌ　9/00	６４１	５Ｂ０８９
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ　13/00	３５１Ｚ	５Ｊ１０４
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｚ	９Ａ００１
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｚ	

審査請求　未請求　請求項の数６　ＯＬ　（全 18 頁）

(21)出願番号　特願平10－340635

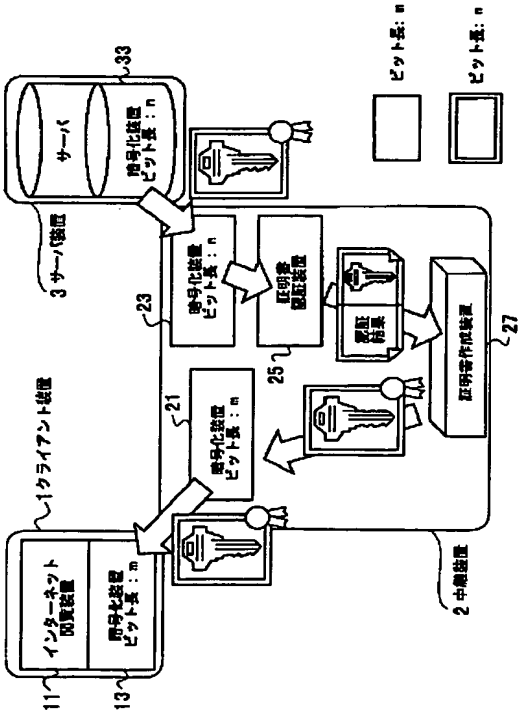
(22)出願日　平成10年11月30日(1998.11.30)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　深澤　広明
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　元田　敏浩
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　100083806
弁理士　三好　秀和　（外１名）

最終頁に続く

(54)【発明の名称】　暗号プロトコル変換装置および方法と暗号プロトコル変換プログラムを記録した記録媒体

(57)【要約】
【課題】　情報の送受信におけるセキュリティを更に強化するとともに通信相手を適確に認証し得る暗号プロトコル変換装置および方法と暗号プロトコル変換プログラムを記録した記録媒体を提供する。
【解決手段】　クライアント装置１とサーバ装置３との間で授受される暗号化情報を中間装置２の暗号化装置２１，２３で更に暗号化しセキュリティを強化するとともに、中間装置２においてサーバ装置３から受信した暗号化情報に付加されている証明書を証明書認証装置２５で認証し、この認証結果に基づき証明書作成装置２７で新たに証明書を作成し、この作成された証明書をクライアント装置１に送信する。



【特許請求の範囲】
【請求項１】　クライアント装置とサーバ装置との間においてネットワークを介して送受信される暗号化情報のセキュリティを強化する暗号プロトコル変換装置であって、
クライアント装置とサーバ装置との間に設けられる中間装置を有し、該中間装置は、
クライアント装置から受信した暗号化情報を更に暗号化しセキュリティを強化してサーバ装置に送信する第１の暗号化手段と、
サーバ装置から受信した暗号化情報を更に暗号化しセキュリティを強化してクライアント装置に送信する第２の暗号化手段と、
サーバ装置から受信した暗号化情報に付加されている証明書を認証鍵で認証する証明書認証手段と、
該証明書認証手段の認証結果に基づき新たに証明書を作成する証明書作成手段と、
該証明書作成手段で作成された証明書を前記第２の暗号化手段で暗号化してクライアント装置に送信する送信手段とを有し、
クライアント装置は、前記認証鍵と同じ認証鍵を有し、該認証鍵で前記中間装置から送信されてくる証明書を認証する認証手段を有することを特徴とする暗号プロトコル変換装置。
【請求項２】　前記証明書作成手段で新たに作成された証明書を保存する証明書保存手段と、
前記証明書認証手段での認証結果に基づき前記証明書保存手段から証明書を検索し、この検索した証明書を前記第２の暗号化手段で暗号化してクライアント装置に返送する返送手段とを更に有することを特徴とする請求項１記載の暗号プロトコル変換装置。
【請求項３】　クライアント装置とサーバ装置との間においてネットワークを介して送受信される暗号化情報のセキュリティを強化する暗号プロトコル変換方法であって、
クライアント装置から受信した暗号化情報を更に暗号化しセキュリティを強化してサーバ装置に送信し、
サーバ装置から受信した暗号化情報を更に暗号化しセキュリティを強化してクライアント装置に送信し、
サーバ装置から受信した暗号化情報に付加されている証明書を認証鍵で認証し、
この認証結果に基づき新たに証明書を作成し、
この作成された証明書を暗号化してクライアント装置に送信し、
クライアント装置は、この送信されてくる証明書を受信し、前記認証鍵と同じ認証鍵で認証することを特徴とする暗号プロトコル変換方法。
【請求項４】　前記新たに作成された証明書を証明書保存手段に保存し、
前記認証結果に基づき前記証明書保存手段から証明書を検索し、この検索した証明書を暗号化してクライアント装置に返送することを特徴とする請求項３記載の暗号プロトコル変換方法。
【請求項５】　クライアント装置とサーバ装置との間においてネットワークを介して送受信される暗号化情報のセキュリティを強化する暗号プロトコル変換プログラムを記録した記録媒体であって、
クライアント装置から受信した暗号化情報を更に暗号化しセキュリティを強化してサーバ装置に送信し、
サーバ装置から受信した暗号化情報を更に暗号化しセキュリティを強化してクライアント装置に送信し、
サーバ装置から受信した暗号化情報に付加されている証明書を認証鍵で認証し、
この認証結果に基づき新たに証明書を作成し、
この作成された証明書を暗号化してクライアント装置に送信し、
クライアント装置は、この送信されてくる証明書を受信し、前記認証鍵と同じ認証鍵で認証することを特徴とする暗号プロトコル変換プログラムを記録した記録媒体。
【請求項６】　前記新たに作成された証明書を証明書保存手段に保存し、
前記認証結果に基づき前記証明書保存手段から証明書を検索し、この検索した証明書を暗号化してクライアント装置に返送することを特徴とする請求項５記載の暗号プロトコル変換プログラムを記録した記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、インターネットやイントラネットに代表されるWWWシステムのサーバ装置において情報を提示する際のセキュリティを強化する暗号プロトコル変換装置および方法に関し、更に詳しくは、クライアント装置とサーバ装置との間においてネットワークを介して送受信される暗号化情報のセキュリティを強化する暗号プロトコル変換装置および方法と暗号プロトコル変換プログラムを記録した記録媒体に関する。
【０００２】
【従来の技術】インターネットやイントラネット等のネットワークを介したクライアント装置とサーバ装置との間における情報の送受信においては、従来、例えば図１９に示すように、クライアント装置１のインターネット閲覧装置１１に付随する暗号化装置１３によってクライアント装置１からの要求情報を暗号化し、そのままサーバ装置３に送信し、またサーバ装置３においても暗号化装置３３で応答情報を暗号化し、同様にそのまま送信している。このような構成は単純であるが、セキュリティが弱いため重要な情報の送受信には不安がある。なお、図１９において、鍵マークは、暗号化された情報を示している。
【０００３】また、この例では、クライアント装置１の

暗号化装置１３でサポートしているビット長はｍビットであり、サーバ装置３の暗号化装置３３でサポートしているビット長はｎビットであって、両者の関係はｍ＜ｎであり、ビット長は合ってなく、クライアント装置１の暗号化装置１３は短いビットで構成されているため、十分な安全性を保てない危険性がある。

【０００４】また、従来の別の例として、図２０および図２１に示すように、クライアント装置１とサーバ装置３との間にビット長ｍをサポートする第１の暗号化装置５１とビット長ｎをサポートする第２の暗号化装置５３を有する中間装置５を設け、この中間装置５でクライアント装置１とサーバ装置３との間の情報を暗号化してセキュリティを更に強化するものがある。

【０００５】このように構成される従来例では、クライアント装置１において暗号化装置１３で暗号化された要求情報は、図２０に示すように、中間装置５の暗号化装置５１，５３でビット長ｎに変換されて暗号化され、サーバ装置３に送信され、これによりセキュリティを強化している。

【０００６】また、サーバ装置３において暗号化装置３３で暗号化され、証明書を付加された応答情報は、図２１に示すように、中間装置５の暗号化装置５１，５３でビット長ｍに変換されて暗号化されて、クライアント装置１に送信され、これによりセキュリティを強化するようになっているが、この場合に前記応答情報は中間装置５で認証されるため、中間装置からクライアント装置へ渡る応答情報は証明書が付加されていない状態にある。従って、クライアント装置が受け取る応答情報の発信元を特定することはできない。

【０００７】なお、図２１において、鍵マークは暗号化された情報を示し、記章マークは証明書付きであることを示している。

【０００８】また、図２２に示すように、一般に流通しているインターネット閲覧装置１１を有するクライアント装置１の暗号化装置１３がサポートするビット長がｍビットであって、サーバ装置３の暗号化装置３３がサポートするビット長ｎと合わない場合には、クライアント装置１の暗号化装置１３をビット長ｎをサポートする暗号化装置１３０に取り替える方法もある。

【０００９】

【発明が解決しようとする課題】上述した従来技術において、図１９で示す方法はセキュリティが弱く、重要な情報の送受信に不安があり、十分な安全性を保つことができないという問題がある。

【００１０】また、図２０、図２２で示す従来技術において、セキュリティの問題は解消し得るが、サーバ装置３から中間装置５へ情報を送信する際、中間装置５で証明書の認証を行ってしまい、クライアント装置１には証明書が送信されないため、クライアント装置１では証明書の認証を行うことができず、従って通信の相手を認証できず、誤った情報がクライアント装置１に送られてもクライアント装置１の方で認証できないという問題がある。

【００１１】本発明は、上記に鑑みてなされたもので、その目的とするところは、情報の送受信におけるセキュリティを更に強化するとともに通信相手を適確に認証し得る暗号プロトコル変換装置および方法と暗号プロトコル変換プログラムを記録した記録媒体を提供することにある。

【００１２】

【課題を解決するための手段】上記目的を達成するため、請求項１記載の本発明は、クライアント装置とサーバ装置との間においてネットワークを介して送受信される暗号化情報のセキュリティを強化する暗号プロトコル変換装置であって、クライアント装置とサーバ装置との間に設けられる中間装置を有し、該中間装置は、クライアント装置から受信した暗号化情報を更に暗号化しセキュリティを強化してサーバ装置に送信する第１の暗号化手段と、サーバ装置から受信した暗号化情報を更に暗号化しセキュリティを強化してクライアント装置に送信する第２の暗号化手段と、サーバ装置から受信した暗号化情報に付加されている証明書を認証鍵で認証する証明書認証手段と、該証明書認証手段の認証結果に基づき新たに証明書を作成する証明書作成手段と、該証明書作成手段で作成された証明書を前記第２の暗号化手段で暗号化してクライアント装置に送信する送信手段とを有し、クライアント装置は、前記認証鍵と同じ認証鍵を有し、該認証鍵で前記中間装置から送信されてくる証明書を認証する認証手段を有することを要旨とする。なお、前記送信手段にあっては、証明書作成手段で作成された証明書をサーバ装置から受信した暗号化情報に付加し、この証明書を付加された暗号化情報を更に前記第２の暗号化手段で暗号化してクライアント装置に送信するものであっても良い。

【００１３】請求項１記載の本発明にあっては、クライアント装置から受信した暗号化情報を更に暗号化しセキュリティを強化してサーバ装置に送信し、サーバ装置から受信した暗号化情報を更に暗号化しセキュリティを強化してクライアント装置に送信し、サーバ装置から受信した暗号化情報に付加されている証明書を認証鍵で認証し、この認証結果に基づき新たに証明書を作成し、この作成された証明書を暗号化してクライアント装置に送信するため、セキュリティが更に強化されるとともに、クライアント装置は通信相手を適確に認証することができる。

【００１４】また、請求項２記載の本発明は、請求項１記載の発明において、前記証明書作成手段で新たに作成された証明書を保存する証明書保存手段と、前記証明書認証手段での認証結果に基づき前記証明書保存手段から証明書を検索し、この検索した証明書を前記第２の暗号

化手段で暗号化してクライアント装置に返送する返送手段とを更に有することを要旨とする。なお、前記返送手段にあっては、サーバ装置から受信した暗号化情報に対して付加された証明書を中間装置が認識した結果を前記証明書保存手段から検索し、この検索した結果、以前作成された証明書が存在するときには、前記証明書作成手段で新たな証明書を作成することなく、前記証明書保存手段に保存されている証明書を暗号化情報に付加し、前記第２の暗号化手段で暗号化してクライアント装置に返送するものであっても良い。

【００１５】請求項２記載の本発明にあっては、新たに作成された証明書を証明書保存手段に保存し、前記認証結果に基づき前記証明書保存手段から証明書を検索し、この検索した証明書を前記第２の暗号化手段で暗号化してクライアント装置に返送するため、２回目以降の接続ではサーバ装置からの証明書を認証した後、証明書を新たに作成する必要がなく、通信速度が速くなり、通信時間を短縮することができる。

【００１６】更に、請求項３記載の本発明は、クライアント装置とサーバ装置との間においてネットワークを介して送受信される暗号化情報のセキュリティを強化する暗号プロトコル変換方法であって、クライアント装置から受信した暗号化情報を更に暗号化しセキュリティを強化してサーバ装置に送信し、サーバ装置から受信した暗号化情報を更に暗号化しセキュリティを強化してクライアント装置に送信し、サーバ装置から受信した暗号化情報に付加されている証明書を認証鍵で認証し、この認証結果に基づき新たに証明書を作成し、この作成された証明書を暗号化してクライアント装置に送信し、クライアント装置は、この送信されてくる証明書を受信し、前記認証鍵と同じ認証鍵で認証することを要旨とする。なお、前記作成された証明書を暗号化してクライアント装置に送信する際に、該証明書をサーバ装置から受信した暗号化情報に付加し、この証明書を付加された暗号化情報をさらに暗号化してクライアント装置に送信するようにしても良い。

【００１７】請求項３記載の本発明にあっては、クライアント装置から受信した暗号化情報を更に暗号化しセキュリティを強化してサーバ装置に送信し、サーバ装置から受信した暗号化情報を更に暗号化しセキュリティを強化してクライアント装置に送信し、サーバ装置から受信した暗号化情報に付加されている証明書を認証鍵で認証し、この認証結果に基づき新たに証明書を作成し、この作成された証明書を暗号化してクライアント装置に送信するため、セキュリティが更に強化されるとともに、クライアント装置は通信相手を適確に認証することができる。

【００１８】請求項４記載の本発明は、請求項３記載の発明において、前記新たに作成された証明書を証明書保存手段に保存し、前記認証結果に基づき前記証明書保存手段から証明書を検索し、この検索した証明書を暗号化してクライアント装置に返送することを要旨とする。なお、証明書を暗号化してクライアント装置に返送する際に、サーバ装置から受信した暗号化情報に対して付加された証明書を中間装置が認識した結果を前記証明書保存手段から検索し、この検索した結果、以前作成された証明書が存在するときには、新たな証明書を作成することなく、証明書保存手段に保存されている証明書を暗号化情報に付加し、前記第２の暗号化手段で暗号化してクライアント装置に返送するようにしても良い。

【００１９】請求項４記載の本発明にあっては、新たに作成された証明書を証明書保存手段に保存し、前記認証結果に基づき前記証明書保存手段から証明書を検索し、この検索した証明書を前記第２の暗号化手段で暗号化してクライアント装置に返送するため、２回目以降の接続ではサーバ装置からの証明書を認証した後、証明書を新たに作成する必要がなく、通信速度が速くなり、通信時間を短縮することができる。

【００２０】また、請求項５記載の本発明は、クライアント装置とサーバ装置との間においてネットワークを介して送受信される暗号化情報のセキュリティを強化する暗号プロトコル変換プログラムを記録した記録媒体であって、クライアント装置から受信した暗号化情報を更に暗号化しセキュリティを強化してサーバ装置に送信し、サーバ装置から受信した暗号化情報を更に暗号化しセキュリティを強化してクライアント装置に送信し、サーバ装置から受信した暗号化情報に付加されている証明書を認証鍵で認証し、この認証結果に基づき新たに証明書を作成し、この作成された証明書を暗号化してクライアント装置に送信し、クライアント装置は、この送信されてくる証明書を受信し、前記認証鍵と同じ認証鍵で認証する暗号プロトコル変換プログラムを記録媒体に記録することを要旨とする。なお、前記作成された証明書を暗号化してクライアント装置に送信する際に、該証明書をサーバ装置から受信した暗号化情報に付加し、この証明書を付加された暗号化情報をさらに暗号化してクライアント装置に送信するようにしても良い。

【００２１】請求項５記載の本発明にあっては、クライアント装置から受信した暗号化情報を更に暗号化しセキュリティを強化してサーバ装置に送信し、サーバ装置から受信した暗号化情報を更に暗号化しセキュリティを強化してクライアント装置に送信し、サーバ装置から受信した暗号化情報に付加されている証明書を認証鍵で認証し、この認証結果に基づき新たに証明書を作成し、この作成された証明書を暗号化してクライアント装置に送信する暗号プロトコル変換プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【００２２】更に、請求項６記載の本発明は、請求項５記載の発明において、前記新たに作成された証明書を証

明書保存手段に保存し、前記認証結果に基づき前記証明書保存手段から証明書を検索し、この検索した証明書を暗号化してクライアント装置に返送する暗号プロトコル変換プログラムを記録媒体に記録することを要旨とする。

【００２３】請求項６記載の本発明にあっては、新たに作成された証明書を証明書保存手段に保存し、前記認証結果に基づき前記証明書保存手段から証明書を検索し、この検索した証明書を前記第２の暗号化手段で暗号化してクライアント装置に返送する暗号プロトコル変換プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。なお、証明書を暗号化してクライアント装置に返送する際に、サーバ装置から受信した暗号化情報に対して付加された証明書を中間装置が認識した結果を前記証明書保存手段から検索し、この検索した結果、以前作成された証明書が存在するときには、新たな証明書を作成することなく、証明書保存手段に保存されている証明書を暗号化情報に付加し、前記第２の暗号化手段で暗号化してクライアント装置に返送するようにしても良い。

【００２４】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。図１は、本発明の一実施形態に係る暗号プロトコル変換方法を実施する暗号プロトコル変換装置の構成を示す図である。同図に示す暗号プロトコル変換装置は、クライアント装置１とサーバ装置３との間においてインターネットやイントラネット等のネットワークを介して送受信される暗号化情報のセキュリティを強化するために、クライアント装置１とサーバ装置３との間に設けられた中間装置２を有する。

【００２５】中間装置２は、クライアント装置１側に設けられ、クライアント装置１の暗号化装置１３がサポートするビット長mに対応するビット長mをサポートする第１の暗号化装置２１、サーバ装置３側に設けられ、クライアント装置１の暗号化装置３３がサポートするビット長nに対応するビット長nをサポートする第２の暗号化装置２３、クライアント装置１から受信した暗号化情報に付加されている証明書を認証する証明書認証装置２５、およびこの認証結果に基づき新たに証明書を作成する証明書作成装置２７を有する。

【００２６】なお、前記第１および第２の暗号化装置１３，２３がサポートするビット長m，nの関係はm＜nであり、クライアント装置１の暗号化装置１３は短いビットで構成されているものであるが、本発明は、これに限定されるものではなく、逆にm＞nの場合にも同様に適用し得るものである。また、図１において、鍵マークは暗号化された情報を示し、記章マークは証明書付きであることを示している。

【００２７】次に、このように構成される実施形態の作用について図２～図１１に示すシーケンスチャートを参照して説明する。なお、図２は図３～図１１に示す一連のシーケンスを１つにまとめたものであり、その内容は図３～図１１に逐次説明するものと同じであるので、以下の説明では図３～図１１に従って順に説明するが、この場合に図２のまとめたシーケンスも参照されたい。

【００２８】まず、図３に示すように、クライアント装置１はサーバ装置３への要求情報を中間装置２に送信すると同時にサーバ装置３への証明書の発行要求情報を中間装置２に送信する。

【００２９】中間装置２は、図４に示すように、クライアント装置１から送信されてきた要求情報および証明書発行要求情報を受信すると、第１の暗号化装置２１および第２の暗号化装置２３を使用して、更に高度な暗号化処理を行う。それから、中間装置２は、図５に示すように、この暗号化された要求情報および証明書発行要求情報をサーバ装置３に送信する。

【００３０】サーバ装置３は、図６に示すように、前記要求情報および証明書発行要求情報を受信すると、これらの要求に基づいて応答情報を証明書付きで中間装置２に送信する。

【００３１】中間装置２は、図７に示すように、前記証明書付き応答情報を受信すると、該情報を証明書認証装置２５に送る。証明書認証装置２５は、該応答情報に付加されている証明書を認証鍵で認証し、この認証結果を図８に示すように証明書作成装置２７に供給する。

【００３２】証明書作成装置２７は、証明書認証装置２５からの認証結果を受け取ると、該認証結果に基づき図９に示すように新たに証明書を作成する。この新たに作成された証明書を付けた応答情報に対して第１の暗号化装置２１および第２の暗号化装置２３で更に高度な暗号化処理を行い、図１０に示すように、中間装置２からクライアント装置１に返送する。

【００３３】クライアント装置１は、中間装置２から証明書付き応答情報を受信すると、中間装置２の認証鍵と同じ認証鍵を使用して、証明書を認証し、この認証結果に基づき応答情報をインターネット閲覧装置１１に供給して表示する。この際、認証に失敗した場合には、インターネット閲覧装置１１は警告を発生する。また、上述した処理において、万が一にも要求した内容と異なった証明書を中間装置２が受け取った場合でも、中間装置２は従来作成される証明書と全く異なった証明書を発行することにより、クライアント装置１で認証する際、警告を発生し誤った情報を受け取ることを防止することができる。

【００３４】その後は、図１１に示すように、クライアント装置１からの要求情報とサーバ装置３から応答情報の授受が中間装置２の第１の暗号化装置２１および第２の暗号化装置２３を介して繰り返し行われる。

【００３５】次に、本発明の他の実施形態について図１２を参照視して説明する。図１２は、他の実施形態に係

る暗号プロトコル変換方法を実施する暗号プロトコル変換装置の構成を示す図であり、同図に示す暗号プロトコル変換装置は、図１に示した実施形態に対して証明書保存装置２９を追加し、これにより証明書保存装置２９で新たに作成した証明書を保存しておき、証明書認証装置２５の認証結果に基づき該証明書保存装置２９から証明書を検索し、この検索した証明書をクライアント装置１に返送することにより新たな証明書を発行する手間を省略し、通信時間を短縮するようにしたものである。

【００３６】このように構成される実施形態の作用について図１３～図１８に示すシーケンスチャートを参照して説明する。なお、図１３は図１４～図１８に示す一連のシーケンスを１つにまとめたものであり、その内容は図１４～図１８に逐次説明するものと同じであるので、以下の説明では図１４～図１８に従って順に説明するが、この場合に図１３のまとめたシーケンスも参照されたい。

【００３７】また、本実施形態の作用のうち、クライアント装置１から情報を送信し、サーバ装置３から証明書付き応答情報を中間装置２に送信するまでの処理は、上述した図３～図６に示す処理と同じであり、その説明は省略して、その続きについて図１４以降を参照して説明する。

【００３８】すなわち、中間装置２は、サーバ装置３から証明書付き応答情報を受信すると、図１４に示すように、該情報を証明書認証装置２５に送る。証明書認証装置２５は、該応答情報に付加されている証明書を認証鍵で認証し、この認証結果を図１５に示すように証明書保存装置２９に供給する。

【００３９】証明書保存装置２９は、図１６に示すように、証明書の認証結果から以前に証明書作成装置２７で作成されたサーバ装置３に関する証明書を検索する。そして、この検索した証明書を付加した応答情報に対して第１の暗号化装置２１および第２の暗号化装置２３で更に高度の暗号化処理を行い、図１７に示すようにクライアント装置１に返送する。

【００４０】その後は、図１８に示すように、クライアント装置１からの要求情報とサーバ装置３から応答情報の授受が中間装置２の第１の暗号化装置２１および第２の暗号化装置２３を介して繰り返し行われる。

【００４１】

【発明の効果】以上説明したように、本発明によれば、クライアント装置とサーバ装置との間で授受される暗号化情報に対して更に高度の暗号化処理を施すとともに、サーバ装置からの暗号化情報に付加されている証明書を認証し、該認証結果に基づき新たに証明書を作成し、この証明書を暗号化してクライアント装置に送信するので、セキュリティが更に強化され、安全性を向上することができるとともに、クライアント装置は通信相手を適確に認証することができる。

【００４２】また、本発明によれば、新たに作成された証明書を証明書保存手段に保存し、認証結果に基づき証明書保存手段から証明書を検索し、この証明書をクライアント装置に返送するので、２回目以降の接続ではサーバ装置からの証明書を認証した後、証明書を新たに作成する必要がなく、通信速度が速くなり、通信時間を短縮することができる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係る暗号プロトコル変換方法を実施する暗号プロトコル変換装置の構成を示す図である。

【図２】図１に示す暗号プロトコル変換装置の全体的作用を示すシーケンス図である。

【図３】図１に示す暗号プロトコル変換装置の処理の一部を示すシーケンス図である。

【図４】図１に示す暗号プロトコル変換装置の処理の一部を示すシーケンス図である。

【図５】図１に示す暗号プロトコル変換装置の処理の一部を示すシーケンス図である。

【図６】図１に示す暗号プロトコル変換装置の処理の一部を示すシーケンス図である。

【図７】図１に示す暗号プロトコル変換装置の処理の一部を示すシーケンス図である。

【図８】図１に示す暗号プロトコル変換装置の処理の一部を示すシーケンス図である。

【図９】図１に示す暗号プロトコル変換装置の処理の一部を示すシーケンス図である。

【図１０】図１に示す暗号プロトコル変換装置の処理の一部を示すシーケンス図である。

【図１１】図１に示す暗号プロトコル変換装置の処理の一部を示すシーケンス図である。

【図１２】本発明の他の実施形態に係る暗号プロトコル変換方法を実施する暗号プロトコル変換装置の構成を示す図である。

【図１３】図２に示す暗号プロトコル変換装置の全体的作用を示すシーケンス図である。

【図１４】図２に示す暗号プロトコル変換装置の処理の一部を示すシーケンス図である。

【図１５】図２に示す暗号プロトコル変換装置の処理の一部を示すシーケンス図である。

【図１６】図２に示す暗号プロトコル変換装置の処理の一部を示すシーケンス図である。

【図１７】図２に示す暗号プロトコル変換装置の処理の一部を示すシーケンス図である。

【図１８】図２に示す暗号プロトコル変換装置の処理の一部を示すシーケンス図である。

【図１９】従来技術におけるクライアント装置とサーバ装置との間における情報の送受信の一例を説明するための図である。

【図２０】従来技術におけるクライアント装置とサーバ

装置との間における情報の送受信の他の例を説明するための図である。

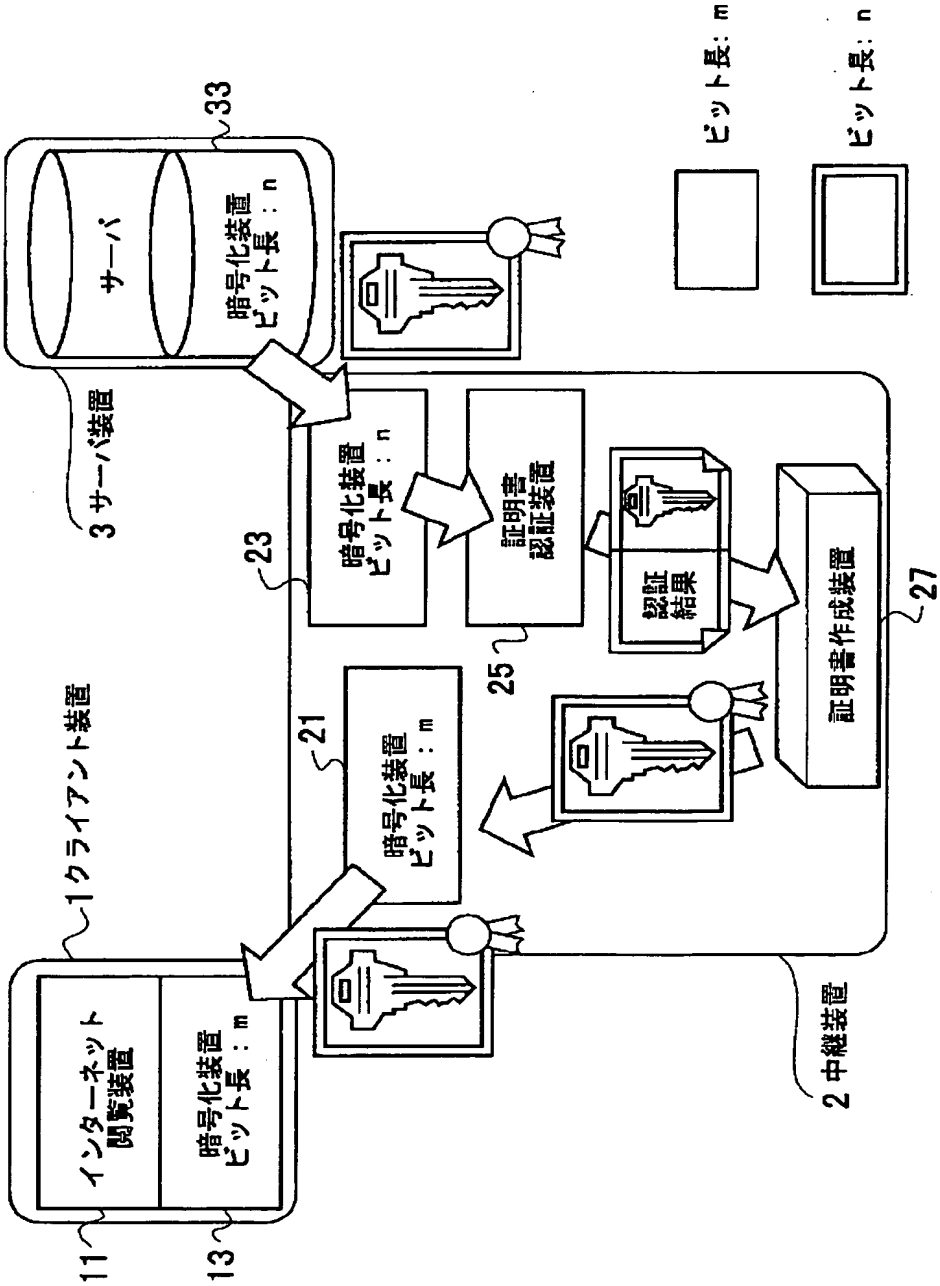
【図２１】図２０の従来技術におけるサーバ装置からクライアント装置への情報の送信を示す図である。

【図２２】従来技術の別の例を示す図である。

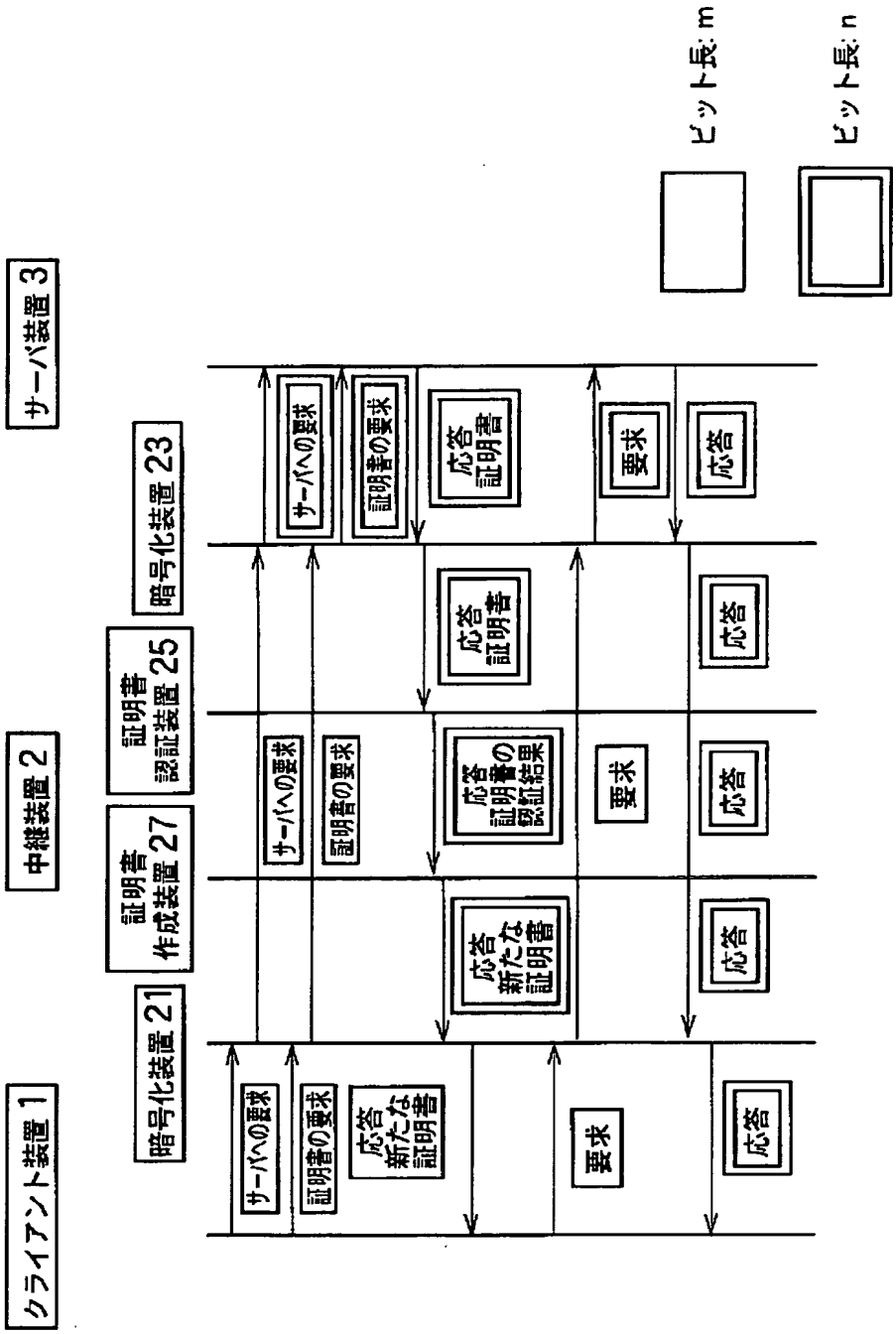
【符号の説明】

１　クライアント装置
２　中間装置
３　サーバ装置
１１　インターネット閲覧装置
１３，３３　暗号化装置
２１　第１の暗号化装置
２３　第２の暗号化装置
２５　証明書認証装置
２７　証明書作成装置
２９　証明書保存装置

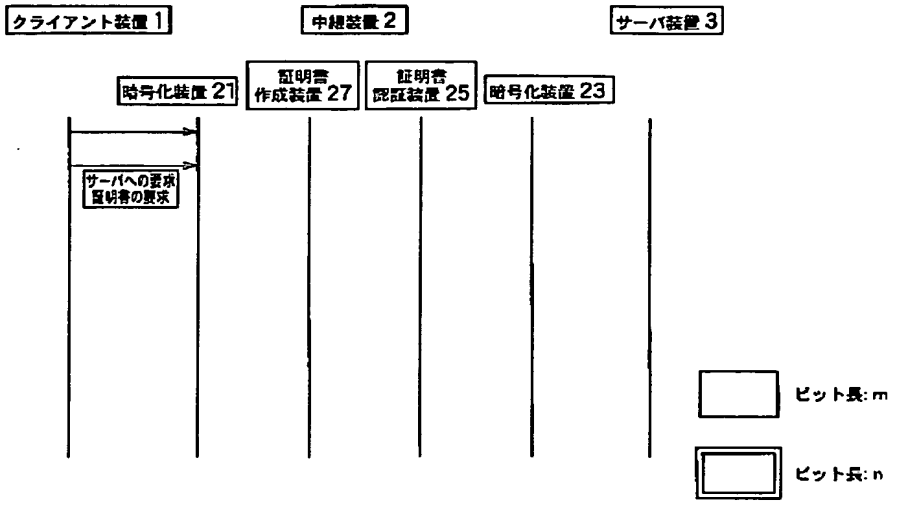
【図１】



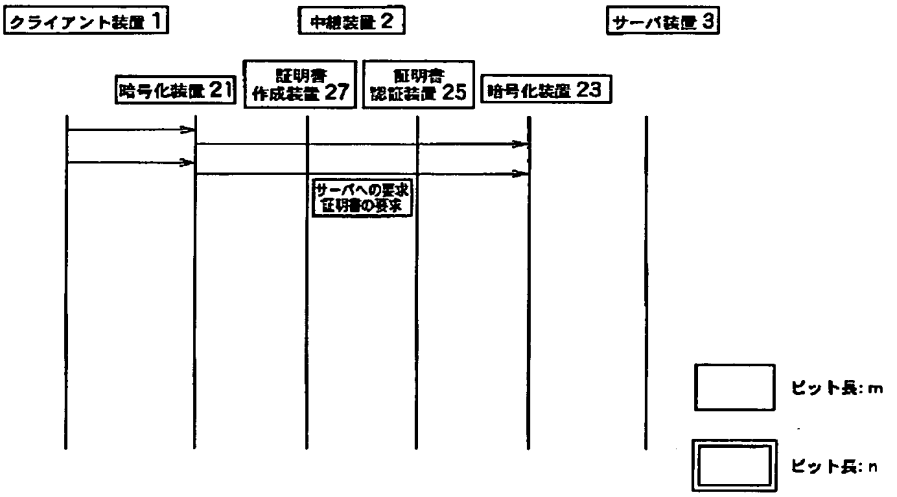
【図２】


ビット長:m
ビット長:n
クライアント装置 1
中継装置 2
サーバ装置 3
暗号化装置 21
証明書作成装置 27
証明書認証装置 25
暗号化装置 23
サーバへの要求
証明書の要求
応答 新たな証明書
要求
応答
サーバへの要求
証明書の要求
応答 証明書の認証結果
要求
応答
応答 新たな証明書
応答
サーバへの要求
証明書の要求
応答 証明書
要求
応答
応答 証明書
応答

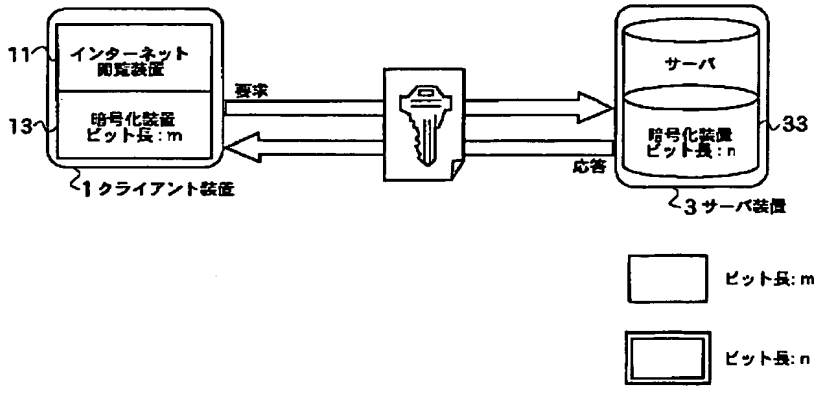
【図３】


クライアント装置 1
中継装置 2
サーバ装置 3
暗号化装置 21
証明書作成装置 27
証明書認証装置 25
暗号化装置 23
サーバへの要求
証明書の要求
ビット長: m
ビット長: n

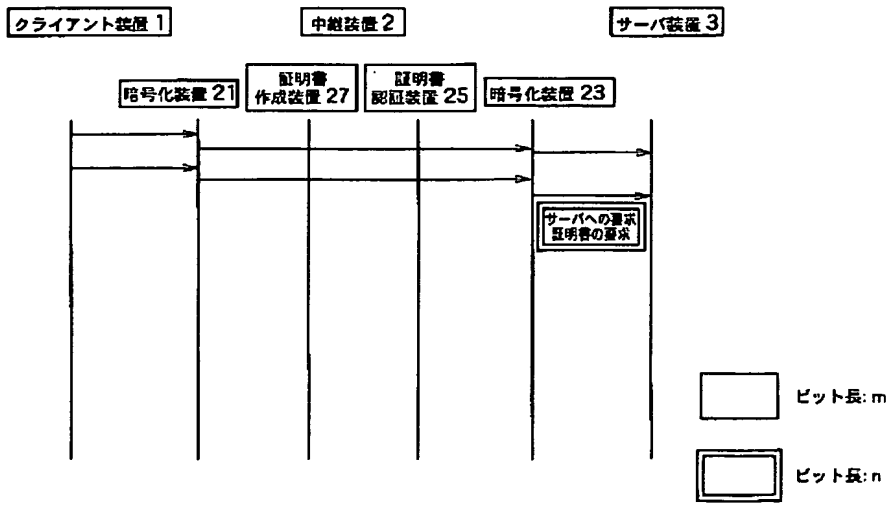
【図４】


クライアント装置 1
中継装置 2
サーバ装置 3
暗号化装置 21
証明書作成装置 27
証明書認証装置 25
暗号化装置 23
サーバへの要求
証明書の要求
ビット長: m
ビット長: n

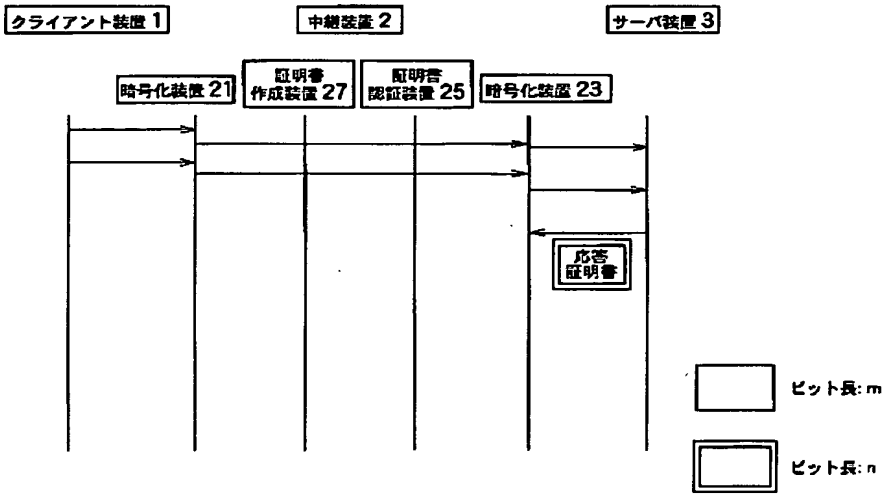
【図１９】


11
インターネット閲覧装置
13
暗号化装置 ビット長: m
1 クライアント装置
要求
応答
サーバ
暗号化装置 ビット長: n
33
3 サーバ装置
ビット長: m
ビット長: n

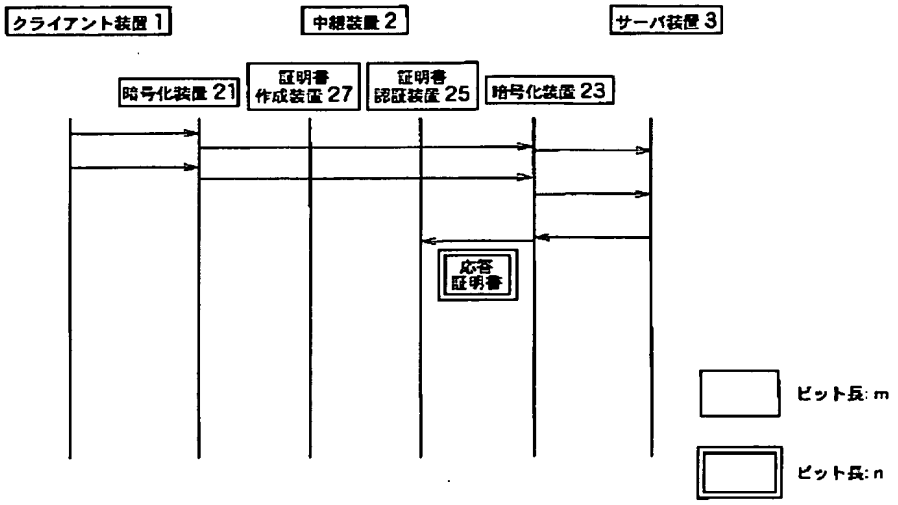
【図５】


クライアント装置 1
中継装置 2
サーバ装置 3
暗号化装置 21
証明書作成装置 27
証明書認証装置 25
暗号化装置 23
サーバへの要求
証明書の要求
ビット長: m
ビット長: n

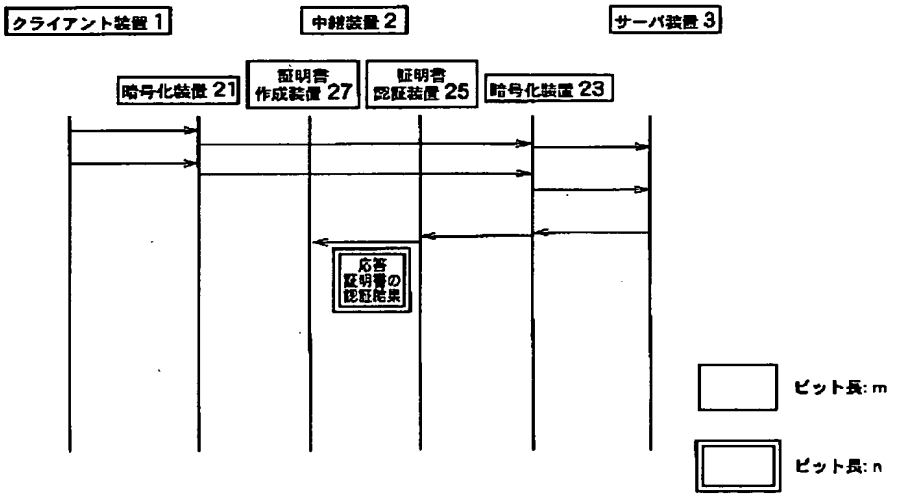
【図６】


クライアント装置 1
中継装置 2
サーバ装置 3
暗号化装置 21
証明書作成装置 27
証明書認証装置 25
暗号化装置 23
応答
証明書
ビット長: m
ビット長: n

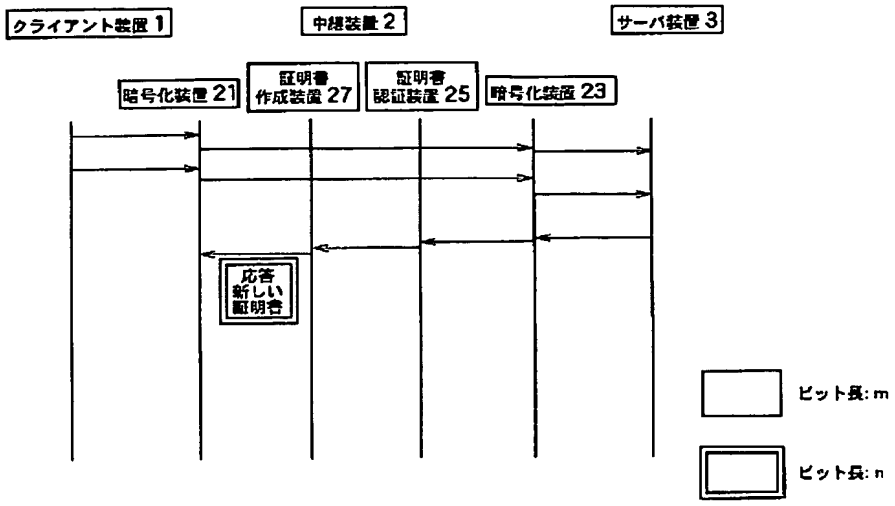
【図７】


クライアント装置 1
中継装置 2
サーバ装置 3
暗号化装置 21
証明書作成装置 27
証明書認証装置 25
暗号化装置 23
応答証明書
ビット長: m
ビット長: n

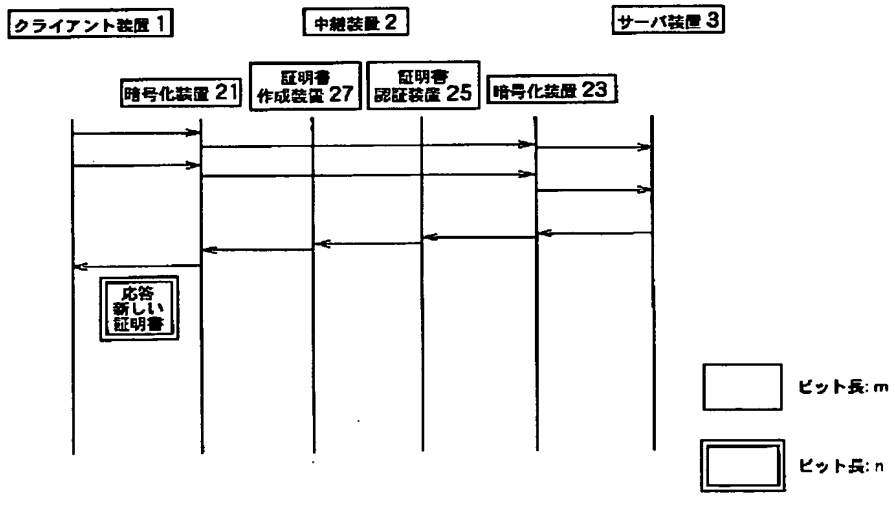
【図８】


クライアント装置 1
中継装置 2
サーバ装置 3
暗号化装置 21
証明書作成装置 27
証明書認証装置 25
暗号化装置 23
応答証明書の認証結果
ビット長: m
ビット長: n

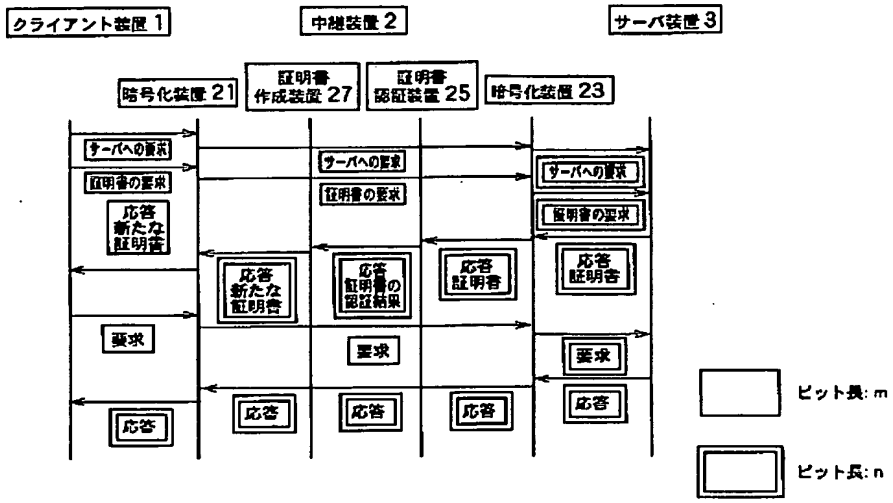
【図９】


クライアント装置 1
中継装置 2
サーバ装置 3
暗号化装置 21
証明書作成装置 27
証明書認証装置 25
暗号化装置 23
応答
新しい
証明書
ビット長: m
ビット長: n

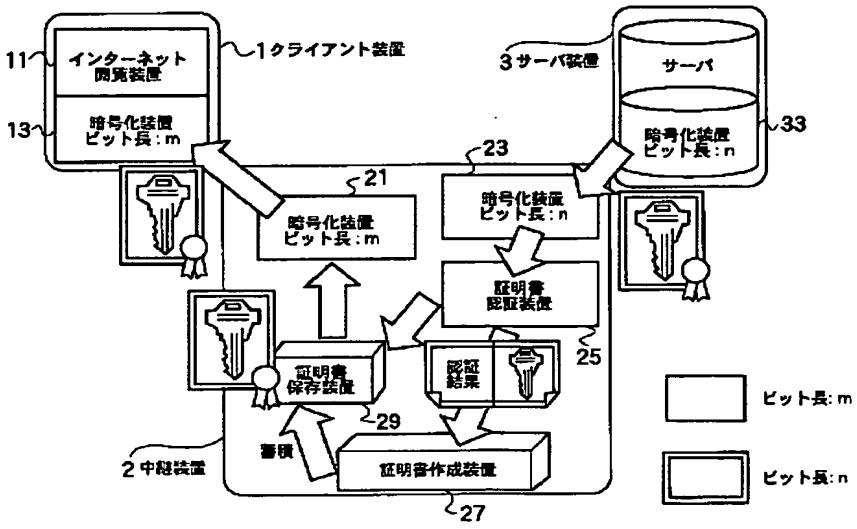
【図１０】


クライアント装置 1
中継装置 2
サーバ装置 3
暗号化装置 21
証明書作成装置 27
証明書認証装置 25
暗号化装置 23
応答
新しい
証明書
ビット長: m
ビット長: n

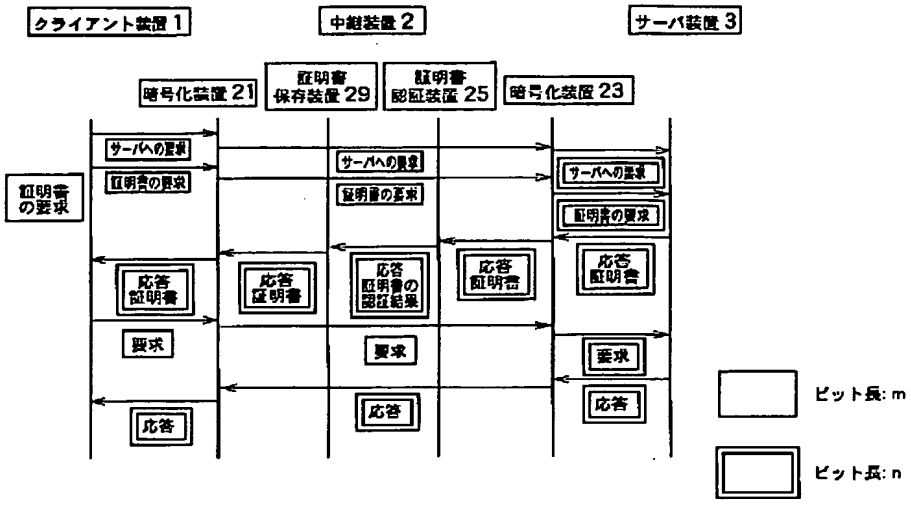
【図１１】


クライアント装置 1
中継装置 2
サーバ装置 3
暗号化装置 21
証明書作成装置 27
証明書認証装置 25
暗号化装置 23
サーバへの要求
証明書の要求
応答 新たな証明書
応答 証明書の認証結果
応答 証明書
要求
応答
ビット長: m
ビット長: n

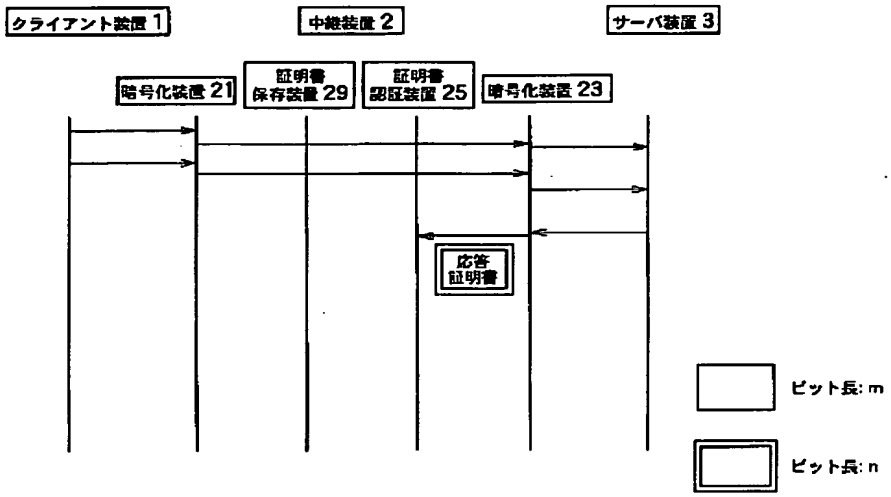
【図１２】


11
インターネット閲覧装置
1クライアント装置
13
暗号化装置 ビット長: m
3サーバ装置
サーバ
33
暗号化装置 ビット長: n
23
21
暗号化装置 ビット長: m
暗号化装置 ビット長: n
証明書認証装置
25
認証結果
証明書保存装置
29
書積
2 中継装置
証明書作成装置
27
ビット長: m
ビット長: n

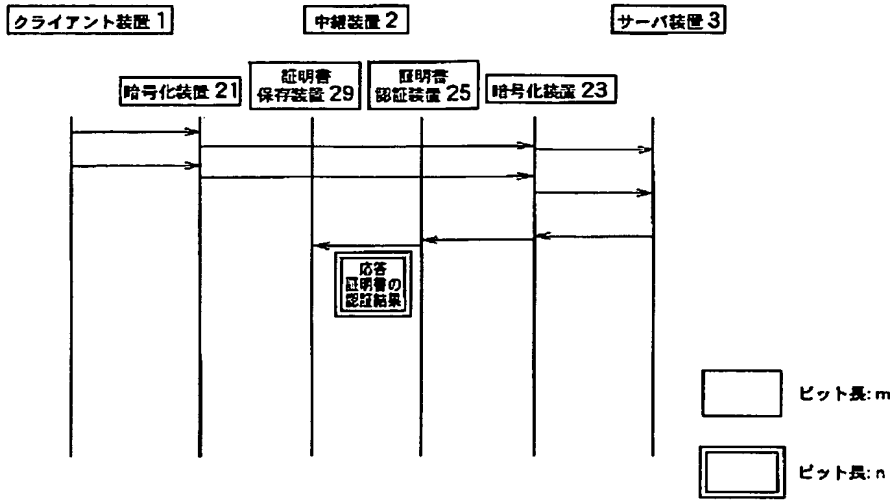
【図１３】


クライアント装置 1
中継装置 2
サーバ装置 3
暗号化装置 21
証明書保存装置 29
証明書認証装置 25
暗号化装置 23
証明書の要求
サーバへの要求
証明書の要求
サーバへの要求
証明書の要求
サーバへの要求
証明書の要求
応答証明書
応答証明書
応答証明書の認証結果
応答証明書
応答証明書
要求
要求
要求
応答
応答
応答
ビット長: m
ビット長: n

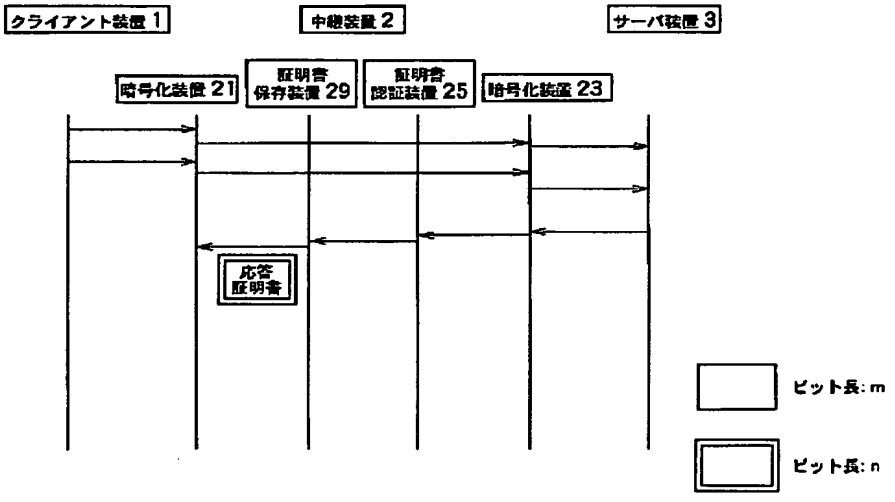
【図１４】


クライアント装置 1
中継装置 2
サーバ装置 3
暗号化装置 21
証明書保存装置 29
証明書認証装置 25
暗号化装置 23
応答証明書
ビット長: m
ビット長: n

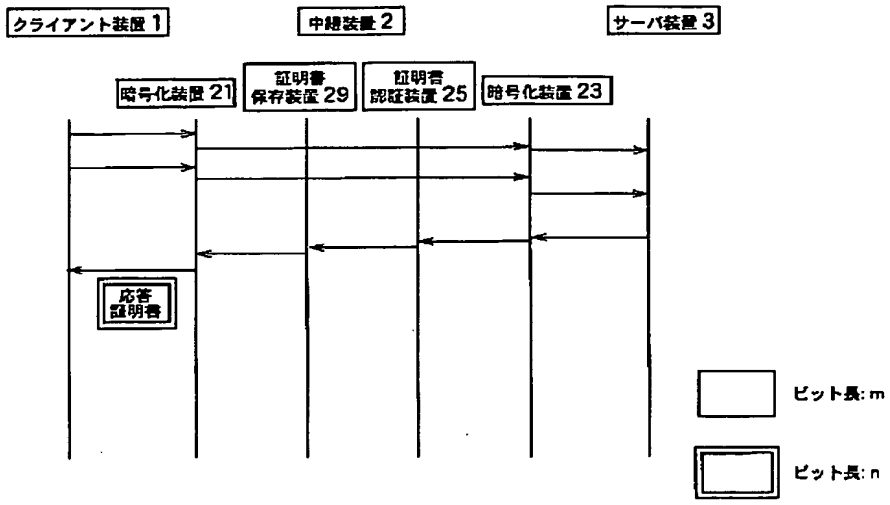
【図１５】


クライアント装置 1
中継装置 2
サーバ装置 3
暗号化装置 21
証明書保存装置 29
証明書認証装置 25
暗号化装置 23
応答証明書の認証結果
ビット長: m
ビット長: n

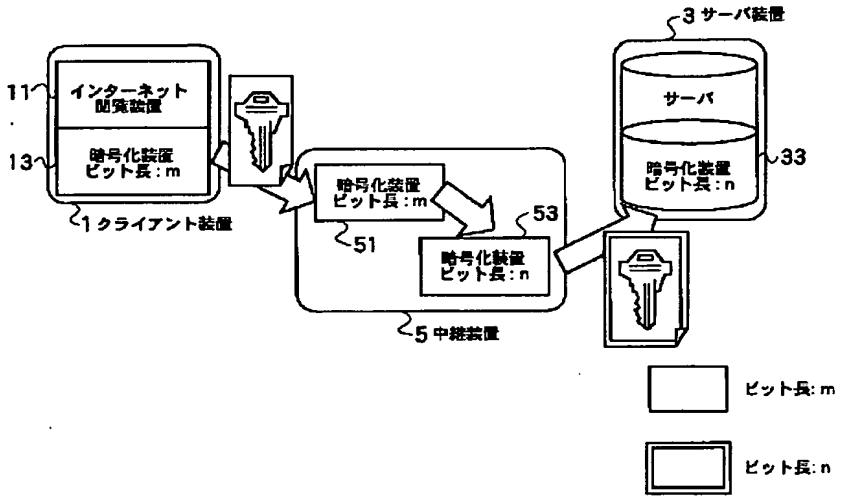
【図１６】


クライアント装置 1
中継装置 2
サーバ装置 3
暗号化装置 21
証明書保存装置 29
証明書認証装置 25
暗号化装置 23
応答証明書
ビット長: m
ビット長: n

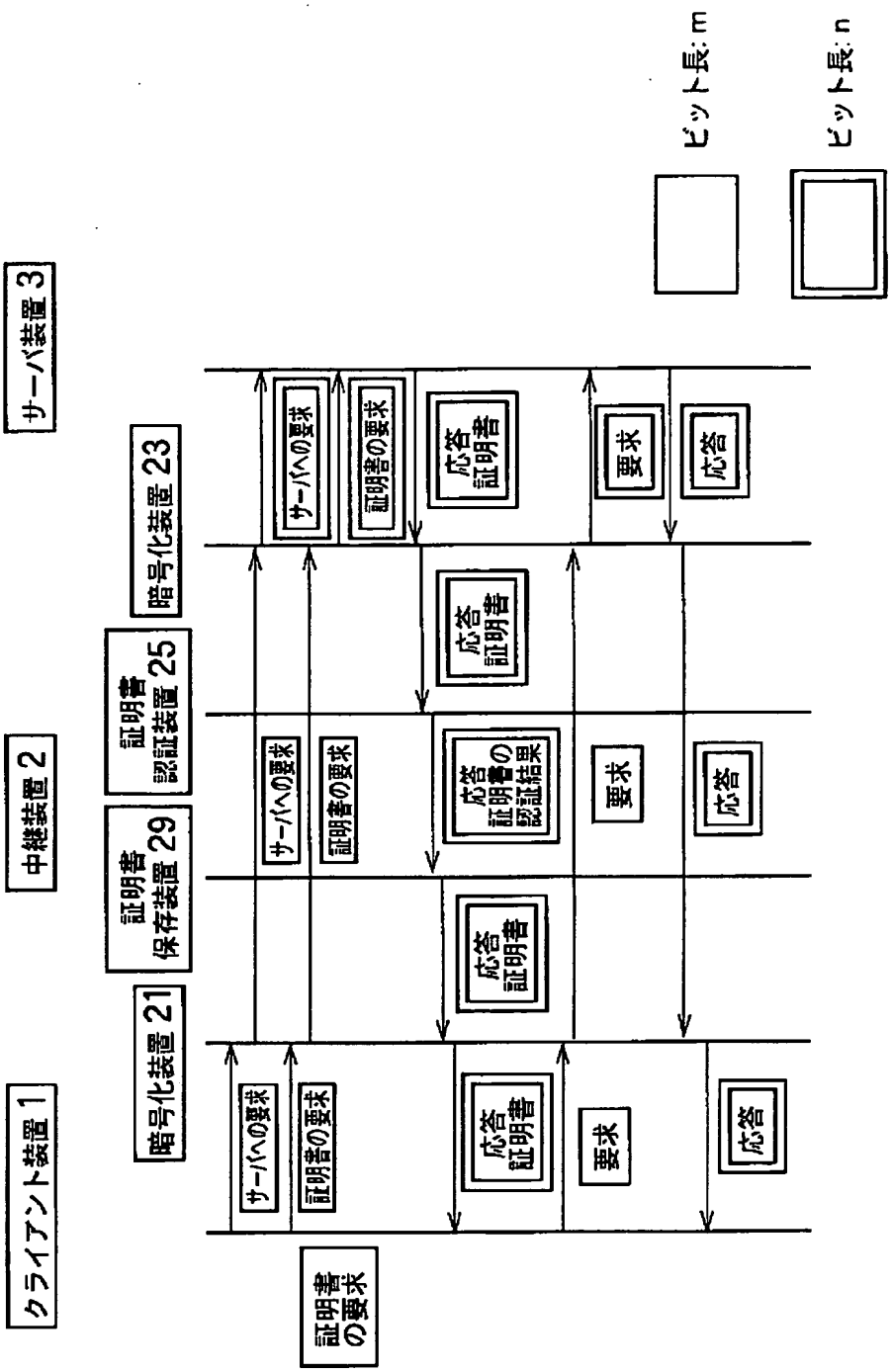
【図１７】


クライアント装置 1
中継装置 2
サーバ装置 3
暗号化装置 21
証明書保存装置 29
証明書認証装置 25
暗号化装置 23
応答証明書
ビット長: m
ビット長: n

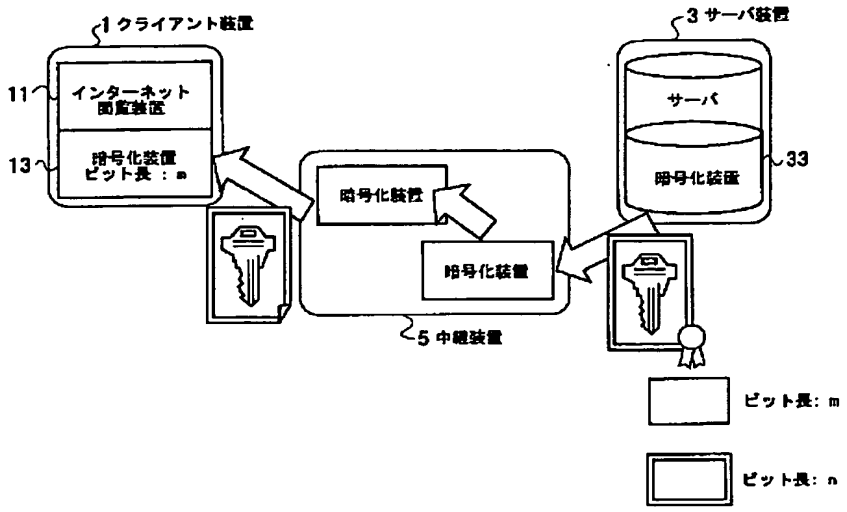
【図２０】


3 サーバ装置
11
インターネット閲覧装置
13
暗号化装置 ビット長 : m
1 クライアント装置
暗号化装置 ビット長 : m
51
53
暗号化装置 ビット長 : n
5 中継装置
サーバ
暗号化装置 ビット長 : n
33
ビット長: m
ビット長: n

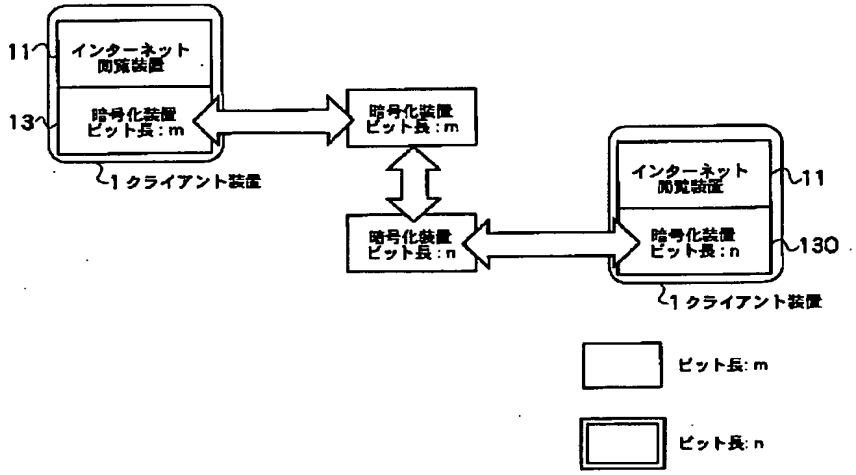
【図１８】


ビット長:m
ビット長:n
クライアント装置 1
中継装置 2
サーバ装置 3
暗号化装置 21
証明書保存装置 29
証明書認証装置 25
暗号化装置 23
証明書の要求
サーバへの要求
証明書の要求
応答証明書
要求
応答
サーバへの要求
証明書の要求
応答証明書
応答証明書の認証結果
要求
応答
サーバへの要求
証明書の要求
応答証明書
応答証明書
要求
応答

【図２１】



【図２２】



フロントページの続き

Ｆターム(参考) 5B089 GA11 GA21 JA00 JB23 KA17
KB13 KC57 KC58 KF05 KH30
5J104 AA01 AA07 KA01 KA04 LA02
PA09
9A001 EE03 JJ25 LL03